

Listing of Claims:

1. (Previously Presented) A method for determining whether a client communication system seeking access to a host communication system is authorized to do so, the method comprising:

receiving, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier;

accessing, at the host, a password;

performing a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system;

comparing results of the first and second mathematical computations; and

designating a client communication system as unauthorized based on the comparison of the results of the first and second mathematical computations,

wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

2. (Previously Presented) The method of claim 1, wherein either the first or second mathematical computations comprises a hashing algorithm.

3. (Previously Presented) The method of claim 1, wherein the first mathematical computation is performed when a communication is initiated.

4. (Original) The method of claim 1, wherein the access password comprises a subscriber password.

5. (Original) The method of claim 1, wherein the access password comprises a user password.

6. (Original) The method of claim 1, wherein the access password comprises an account password.

7. (Canceled)

8. (Original) The method of claim 1, wherein the client-communication-system-specific identifier comprises a device-specific identifier.

9. (Original) The method of claim 8, wherein the device-specific identifier comprises a hard disk identifier.

10. (Original) The method of claim 8, wherein the device-specific identifier comprises an Ethernet address.

11. (Original) The method of claim 8, wherein the device-specific identifier comprises a central processing unit serial number.

12. (Original) The method of claim 8, wherein the device-specific identifier comprises a description of the storage characteristics of the hard disk.

13-15. (Canceled)

16. (Previously Presented) The method of claim 1, further comprising sending a notification to the client communication system indicating the designation of the client communication system as an unauthorized client communication system if the result of the first

mathematical computation does not correspond to the result of the second mathematical computation.

17. (Previously Presented) The method of claim 1, further comprising terminating communications from the client communication system if the result of the first mathematical computation does not correspond to result of the second mathematical computation.

18. (Previously Presented) The method of claim 17, wherein terminating communications is performed after a predetermined delay if the result of the first mathematical computation does not correspond to the result of the second mathematical computation.

19. (Previously Presented) A method for handling information about an authorized client communication system, the method comprising:

- storing a version of an access password;

- storing a client-communication-system-specific identifier and results of a first mathematical computation performed, at a client communication system, on the access password and the client-communication-system-specific identifier from the client communication system retrieved from a client communication system;

- performing a second mathematical computation on the stored access password and the retrieved client-communication-system-specific identifier, and

- storing the results of the second mathematical computation,

- wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

20. (Previously Presented) The method of claim 19, wherein:

- storing the result of the first mathematical computation comprises storing the result on the client communication system,

storing the a version of an access password comprises storing the access password on the host communication system.

21. (Canceled)

22. (Previously Presented) The method of claim 19, wherein either the first or second mathematical computations comprises a hashing algorithm.

23. (Original) The method of claim 19, wherein the access password comprises a subscriber password.

24. (Original) The method of claim 19, wherein the access password comprises a user password.

25. (Original) The method of claim 19, wherein the access password comprises an account password.

26. (Canceled)

27. (Original) The method of claim 19, wherein the client-communication-system-specific identifier comprises a device-specific identifier.

28. (Original) The method of claim 27, wherein the device-specific identifier comprises a hard disk identifier.

29. (Original) The method of claim 27, wherein the device-specific identifier comprises an Ethernet address.

30. (Original) The method of claim 27, wherein the device-specific identifier comprises a central processing unit serial number.

31. (Original) The method of claim 27, wherein the device-specific identifier comprises a description of the storage characteristics of the hard disk.

32. (Previously Presented) A computer readable medium or propagated signal having embodied thereon a computer program for identifying an unauthorized client communication system seeking access to a host communication system, the computer program comprising:

- a performing code segment for performing a first mathematical computation on an access password and a client-communication-system-specific identifier;

- a receiving code segment for receiving, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier;

- a received code segment for retrieving, at the host, a password;

- a performing code segment for performing a second mathematical computation using the received password and the client-communication-system-specific identifier received from the client communication system;

- comparing results of the first and second mathematical computations; and

- a designating code segment for designating a client communication system as unauthorized based on a results of the first and second mathematical computations,

wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

33. (Previously Presented) The medium of claim 32, wherein either the first or second mathematical computations comprises a hashing algorithm.

34. (Previously Presented) The medium of claim 32, wherein the performing code segment performs the first mathematical computation when a communication is initiated.

35. (Original) The medium of claim 32, wherein the access password comprises a subscriber password.

36. (Original) The medium of claim 32, wherein the access password comprises a user password.

37. (Original) The medium of claim 32, wherein the access password comprises an account password.

38. (Canceled)

39. (Original) The medium of claim 32, wherein the client-communication-system-specific identifier comprises a device-specific identifier.

40. (Original) The medium of claim 39, wherein the device-specific identifier comprises a hard disk identifier.

41. (Original) The medium of claim 39, wherein the device-specific identifier comprises an Ethernet address.

42. (Original) The medium of claim 39, wherein the device-specific identifier comprises a central processing unit serial number.

43. (Original) The medium of claim 39, wherein the device-specific identifier comprises a description of the storage characteristics of the hard disk.

44-46. (Canceled)

47. (Previously Presented) The medium of claim 32, further comprising a notification code segment for sending a notification to the client communication system indicating the designation of the client communication system as an unauthorized client communication system if the result of the first mathematical computation does not correspond to the result of the second mathematical computation.

48. (Previously Presented) The medium of claim 32, further comprising a terminating code segment for terminating communications from the client communication system if the result of the first mathematical computation does not correspond to result of the second mathematical computation.

49. (Original) The medium of claim 48, wherein the terminating code segment terminates communications after a predetermined delay if the result of the first mathematical computation does not correspond to the result of the host-based mathematical computation.

50. (Previously Presented) A computer readable medium or propagated signal having embodied thereon a computer program for handling information about an authorized client communication system, the computer program comprising:

- an access password storing code segment for storing a version of an access password;;
- a storing code segment for storing, at the host, a client-communication-system-specific identifier and results of a first mathematical computation performed on the access password and the client-communication-system-specific identifier from the client communication system retrieved from a client communication system;
- a performing code segment for performing a second mathematical computation on the stored access password and the retrieved client-communication-system-specific identifier;; and

a computation storing code segment for storing a-the results of the second mathematical computations,

wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

51. (Previously Presented) The medium of claim 50, wherein the performing code segment includes:

a computation storing code segment for storing the result of the first mathematical computation comprises storing the result on the client communication system,

an access password storing code segment to store the version of an access password comprises storing the result on the host communication system.

52. (Canceled)

53. (Previously Presented) The medium of claim 50, wherein either the first or second mathematical computations comprises a hashing algorithm.

54. (Original) The medium of claim 50, wherein the access password comprises a subscriber password.

55. (Original) The medium of claim 50, wherein the access password comprises a user password.

56. (Original) The medium of claim 50, wherein the access password comprises an account password.

57. (Canceled)



58. (Previously Presented) The medium of claim 50, wherein the client communication system-specific identifier comprises a device-specific identifier.

59. (Original) The medium of claim 58, wherein the device-specific identifier comprises a hard disk identifier.

60. (Original) The medium of claim 58, wherein the device-specific identifier comprises an Ethernet address.

61. (Original) The medium of claim 58, wherein the device-specific identifier comprises a central processing unit serial number.

62. (Original) The medium of claim 58, wherein the device-specific identifier comprises a description of the storage characteristics of the hard disk.

63. (Previously Presented) An apparatus for identifying an unauthorized client communication system seeking access to a host communication system, the apparatus comprising:

- a performing device structured and arranged to perform, at a client, a first mathematical computation on an access password and a client-communication-system-specific identifier;

- a receiving device structured and arranged to receive, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier;

- an accessing device structured and arranged to access, at the host, a password;

- a performing device structured and arranged to perform a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system;

a comparing device structured and arranged to compare results of the first and second mathematical computations; and

a designating device structured and arranged to designate a client communication system as unauthorized based on a-the results of the first and second mathematical computations,

wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

64. (Previously Presented) The apparatus of claim 63, wherein either the first or second mathematical computations comprises a hashing algorithm.

65. (Previously Presented) The apparatus of claim 63, wherein the first mathematical computation is performed when a communication is initiated.

66. (Original) The apparatus of claim 63, wherein the access password comprises a subscriber password.

67. (Original) The apparatus of claim 63, wherein the access password comprises a user password.

68. (Original) The apparatus of claim 63, wherein the access password comprises an account password.

69. (Canceled)

70. (Original) The apparatus of claim 63, wherein the client-communication-system-specific identifier comprises a device-specific identifier.

71. (Original) The apparatus of claim 70, wherein the device-specific identifier comprises a hard disk identifier.

72. (Original) The apparatus of claim 70, wherein the device-specific identifier comprises an Ethernet address.

73. (Original) The apparatus of claim 70, wherein the device-specific identifier comprises a central processing unit serial number.

74. (Original) The apparatus of claim 70, wherein the device-specific identifier comprises a description of the storage characteristics of the hard disk.

75-77. (Canceled)

78. (Previously Presented) The apparatus of claim 63, further comprising a device structured and arranged to terminate communications from the client communication system if the result of the first mathematical computation does not correspond to result of the second mathematical computation.

79. (Previously Presented) An apparatus for handling information about an authorized client communication system, the apparatus comprising:

an access password device structured and arranged to store a version of an access password;

a receiving device structured and arranged to receive, at the host, from the client communication system, a client-communication-system-specific identifier and results of a first mathematical computation performed at the client on an access password and the client-communication-system-specific identifier;

an accessing device structured and arranged to access, at the host, a password;

a performing device structured and arranged to perform a second mathematical computation using the accessed password and the client-communication-system-specific identifier received from the client communication system;

a comparing device structured and arranged to compare results of the first and second mathematical computations; and

a performing device structured and arranged to perform a second mathematical computation on the stored access password and the retrieved client-communication-system-specific identifier; and

a computation storing device structured and arranged to store the results of the second mathematical computations,

wherein the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

80. (Previously Presented) The apparatus of claim 79, wherein the performing device includes:

a device for storing the result of the first mathematical computation comprises storing the result on the client communication system,

an access password storing device for storing the version of an access password comprises storing the result on the host communication system.

81-82. (Canceled)

83. (Previously Presented) The apparatus of claim 79, wherein either the first or second mathematical computations comprises a hashing algorithm.

84. (Original) The apparatus of claim 79, wherein the access password comprises a subscriber password.

85. (Original) The apparatus of claim 79, wherein the access password comprises a user password.

86. (Original) The apparatus of claim 79, wherein the access password comprises an account password.

87. (Canceled)

88. (Original) The apparatus of claim 79, wherein the client-communication-system-specific identifier comprises a device-specific identifier.

89. (Original) The apparatus of claim 88, wherein the device-specific identifier comprises a hard disk identifier.

90. (Original) The apparatus of claim 88, wherein the device-specific identifier comprises an Ethernet address.

91. (Original) The apparatus of claim 88, wherein the device-specific identifier comprises a central processing unit serial number.

92. (Original) The apparatus of claim 88, wherein the device-specific identifier comprises a description of the storage characteristics of the hard disk.